МАГІСТЕРСЬКА РОБОТА

ЛОМАКО ОЛЕКСАНДРА ОЛЕКСАНДРОВИЧА

2022 р.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО

Декан факультету
Інформаційних технологій
_____ Глазунова О.Г., д.пед.н, проф.
підпис ПІБ, вчене звання і ступінь

«___»_____2022 р.

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри
Комп'ютерних систем, мереж та кібербезпеки
_____ Касаткін Д. Ю., к.п.н., доц
підпис ПІБ, вчене звання і ступінь

«___»_____2022 р.

МАГІСТЕРСЬКА РОБОТА

На тему: «Розробка та дослідження автоматизованої системи для побудови моделі порушника інформаційної безпеки підприємства»

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма Комп'ютерні системи та мережі

Орієнтація освітньої програми _____

Керівник магістерської роботи: _____ / Лахно В.А. /
підпис ПІБ

Виконав: _____ / Ломако О.О. /
підпис ПІБ

КИЇВ-2022

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
Комп'ютерних систем, мереж та кібербезпеки
_____ / Касаткін Д. Ю., к.п.н., доц. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 20__ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ

Ломако Олександр Олександрович
(прізвище, ім'я, по батькові)
Спеціальність (напрям підготовки): комп'ютерна інженерія
Освітня програма: комп'ютерні системи та мережі
Орієнтація освітньої програми: _____

Тема магістерської роботи: «Розробка та дослідження автоматизованої системи для побудови моделі порушника інформаційної безпеки підприємства»

затверджена наказом ректора НУБіП України від "__" _____ 20__ р. №____
Термін подання завершеної роботи на кафедру _____
Вихідні дані до магістерської роботи _____

Перелік питань, що підлягають дослідженню:
1. Аналітичний огляд
2. Вимоги до мережі
3. Мережева безпека обчислювальної мережі

Перелік графічного матеріалу (за потреби) _____

Дата видачі завдання "__" _____ 2021 р.

Керівник магістерської роботи _____ Лахно В.А., д.т.н., проф.
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Ломако О.О.
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз предметної області		Виконано
2	Визначення вимог для мережі		Виконано
3	Дослідження безпеки мережі		Виконано
4	Оцінка ризиків мережі		Виконано
5	Оформлення пояснювальної записки		Виконано
6	Оформлення графічного матеріалу		Виконано

Студент _____ _____

(підпис) (ініціали та прізвище)

Керівник проекту (роботи) _____ _____

РЕФЕРАТ

Пояснювальна записка: 65 сторінок, 15 рисунків, 9 таблиць, 31 джерело.

АВТОМАТИЗОВАНА СИСТЕМА, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, СИСТЕМА РОЗМЕЖУВАННЯ ДОСТУПУ, ОПЕРАЦІЙНА СИСТЕМА, БЕЗПЕКА

Предметом дослідження є автоматизована система побудови моделей порушників.

Об’єкт дослідження – процес побудови моделей порушника.

Мета роботи – розробка власної автоматизованої системи побудови моделі порушника для підприємств.

Завданнями магістерської роботи є запобігання можливих загроз для комп’ютерної мережі Національного університету біоресурсів і природокористування України .

Перший розділ присвячений аналізу предметної області.

У другому розділі описуються процес розробки системи побудови моделі порушника.

Третій розділ присвячений перевірці роботи системи.

Результати досягнуті в процесі роботи – було розроблено та проведено тестування автоматизованої системи побудови моделей порушників.

Одержані результати можуть бути використані у усіх підприємствах, адже дані дослідження є універсальними.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ОС – операційна система;

ІзОД – інформація з обмеженим доступом

ПРД – правила розмежування доступу.

СРД – система розмежування доступу.

ПЕМВН – канал побічних електромагнітних випромінювань і навідів

ВСТУП

Актуальність. З переходом в інформаційну епоху найважливішим ресурсом стала інформація. Сьогоднішні механізми забезпечення інформаційної безпеки швидко застарівають, і більш кваліфіковані хакери і порушники мають змогу обійти захисні засоби, які використовуються більшістю організацій та компаній. [11]

У минулому використання комп'ютерів в мережі було безпечне, коли використовувалися антивірусні, мережеві екрани та засоби запобігання вторгнення. Але це вже не стосується сучасного складного сценарію загрози, і особливо це стосується великих організацій, які мають дуже складні та великі інфраструктури.

Саме з цим пов'язане збільшення кількості інформаційних протистоянь, а витрати від такого протистояння не тільки залишаються незмінними, а навпаки —зростають.

Інформація – відомості про об'єкти та явища навколишнього середовища, їхні параметри, властивості й стани, які зменшують наявну про них ступінь невизначеності, неповноти знань.

Рис. 1. Об'єм втрати даних 2005-

Інформацію можна розглядати як концептуально зв'язані між собою відомості, дані, поняття, що змінюють уявлення про явище або об'єкт навколишнього світу. Поряд з інформацією часто використовують поняття дані. Дані можуть розглядатися як ознаки або записані спостереження, які з будь яких причин не використовуються, а тільки зберігаються. У тому випадку, якщо з'являється можливість використати ці

дані для визначення невизначеності будь-чого, дані перетворюються в інформацію. Тобто інформація – це дані, які використовуються.[1-3]

Для ведення ефективної боротьби та для ефективного захисту інформації фахівцями було розроблено та запропоновано різні види моделей, зокрема, для початкового прогнозування ризиків і втрат пов'язаних із веденням інформаційного протиборства. Такі моделі дозволяють із заданою точністю відобразити сам процес і, що є найголовнішим, його наслідки. Визначившись із ресурсами котрими володітиме сторона нападу, наступним кроком буде перехід до моделювання ситуації динамічного протистояння, коли одна із сторін буде реагувати на дії іншої, таким чином зменшуючи втрати від інформаційного протистояння.

Модель порушника представляє собою опис можливих дій порушника, який складається на підставі детального аналізу можливих загроз, способів та каналів їх реалізації, а також типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей.

Модель порушника носить неформальний характер, і, як наслідок, не існує строго однозначної методики зі складання такої. Безліч авторів у науково-технічній літературі визначає різні способи класифікації порушників, тим часом багато фахівців з інформаційної безпеки, які працюють на підприємствах, змушені складати свої нормативно-методичні документи, тому що існуючі моделі далеко не завжди задовольняють усім особливостям роботи організації. Незважаючи на те що багато моделей мають високий рівень кореляції між класифікаційними признаками, виробити єдину модель досі не вдалося. [11-13]

Метою роботи є розробка власної автоматизованої системи побудови моделі порушника для підприємств.

Для досягнення мети необхідно виконати наступні дії:

- Проаналізувати існуючі автоматизовані системи побудови моделей;
- Дослідити моделі порушника і способи побудови моделей;
- Розробити автоматизовану систему побудови моделі порушника

- Провести експериментальне дослідження автоматизованої системи для перевірки коректності її роботи

Об'єкт дослідження – процес побудови моделей порушника

Предмет дослідження – автоматизована система побудови моделей

Для отримання інформації, на основі якої будуть проводитися заходи по розробці автоматизованої системи, необхідно провести дослідження відповідної літератури, пов'язаної з моделлю порушника, видами моделей, а також методами побудови моделей порушника та. Відповідно до отриманої інформації можна робити систему побудови моделі порушника.

Новизна - удосконалено процес побудови моделі порушника, що за рахунок автоматизації результатів анкетування підприємства, можливості вибору АС різних класів та використання україномовного інтерфейсу дозволяє спростити процес побудови КСЗІ на підприємстві

Практична цінність розробки є створення автоматизованої системи, якій немає аналогів, завдяки якій спрощується процедура побудови моделі порушника

РОЗДІЛ 1
АНАЛІЗ МОДЕЛІ ПОРУШНИКА ТА ЇЇ ВИДИ

1.1. Характеристика моделі порушника

Модель порушника – це опис можливих дій зловмисника, що формується на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Необхідно будувати модель порушника для розробки комплексу заходів для забезпечення безпеки алгоритму. Така модель може бути заснована на різних критеріях.

Побудова моделі порушника робиться для отримання відповідей на такі питання:

1. Від кого захищатиметься інформація?
2. Яка ціль у порушника?
3. Якими знаннями володіє порушник?
4. Які повноваження в системі має можливий порушник?
5. Які методи і засоби може використовувати порушник? [13]

Під ймовірнісною моделлю [stochastic, probabilistic model] – розуміють модель, яка на відміну від детермінованої моделі містить випадкові елементи. При заданні на вході моделі деякої сукупності значень, на її виході можуть отримуватися різні між собою результати в залежності від дії випадкового фактора. [9]

Під математичною моделлю порушника розуміється модель, яка містить випадкові елементи у вигляді ймовірностей успішного виконання окремих атак, які формують одну загальну атаку, і визначає ймовірність досягнення кінцевої цілі цієї атаки порушником.

Щоб модель порушника була максимально корисною – вона повинна орієнтуватися на конкретний об’єкт захисту. Тому модель не може бути універсальною і синтезується виходячи з аналізу структури системи, ресурсів і способів їх використання. [10-11]

Практично кожна інформаційна система містить таку інформацію, розголошення якої третім особам може завдати шкоди власнику або особі, до якої ця інформація відноситься. Тема інформаційної безпеки особливо актуальна в компаніях і організаціях, які обробляють інформацію з обмеженим доступом. Одним із етапів побудови інтегрованої системи інформаційної безпеки є розробка моделі зловмисника. Чим точніше буде визначено зображення, алгоритм дій потенційного зловмисника, тим легше адміністраторам безпеки буде розробити набір заходів для запобігання успішним атакам. Важливу роль у розвитку моделі правопорушника відіграє вибір класифікації правопорушників. Тому, щоб якомога точніше ідентифікувати правопорушників, збитки від яких будуть максимальними, необхідно класифікувати всі види суб'єктів, які мають потенціал взаємодії з джерелами інформації, за всіма можливими для системи показниками, які дуже важливо спростити цю процедуру.

Порушників поділяють на зовнішні та внутрішні. Внутрішні працівники — це працівники, користувачі інформаційної системи, які можуть завдати шкоди джерелам інформації як ненавмисно, так і навмисно; технічний персонал будівель і прибудинкових територій (електрики, сантехніки, прибиральники тощо); Персонал, що обслуговує технічні ресурси (інженери, техніки). Зовнішні зловмисники – це сторонні особи, які перебувають за межами контрольованої зони організації або не уповноважені використовувати цю комп'ютерну систему. Це означає, що вони не мають облікового запису в системі і відповідно до політики безпеки системи вони взагалі не можуть працювати в цій системі. Приклади сторонніх зловмисників: відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих обмежень; досвідчені хакери; особи, найняті конкурентами для отримання необхідної інформації; порушник доступу.

Розробляючи модель зловмисника, необхідно визначити, що і в якій мірі має відображати отримана модель. Для цього необхідно визначити необхідний рівень деталізації моделі зловмисника. [1-3]

1.2. Методика побудови моделі порушника

Порушником можна розглядати особу, що прагне чи може одержати несанкціонований доступ до роботи з включеними до складу АС засобами. При побудові моделі порушника необхідно враховувати, що особливістю ресурсів АС, особливо інформаційних - є їх принадливість для окремих осіб чи певних груп осіб, які з ціллю використання цих ресурсів є користувачами автоматизованої системи, чи намагаються ними стати. Ця принадливість найчастіше є обумовленою характером та об'ємом інформації, яка вводиться, обробляється, зберігається та циркулює в системах АС. Якщо якась особа – користувач ресурсами АС здійснює спробу несанкціонованого доступу до об'єктів захисту (ознайомлення, модифікація, знищення, зміна режимів використання чи функціонування тощо), то такий користувач являтиметься порушником.

По відношенню до АС порушники можуть бути внутрішніми (співробітники підприємства, користувачі системи) чи зовнішніми (сторонні особи, чи будь-які особи, що знаходяться за межами контрольованої зони).

Під зовнішніми порушниками для інформаційної системи необхідно розуміти в першу чергу конкуруючі організації, а також потенційні терористичні / кримінальні угруповання, також ними можуть буду потенційні корупційні елементи, що знаходяться в органах влади.

Вірогідніше діяльність даних порушників спрямована першочергово на будь-які пасивні носії, копіювання, псування або знищення її носіїв.

Також дії зовнішніх порушників може бути спрямована на персонал, і може проявлятися у вигляді різних загроз або підкупу співробітників, з метою отримання необхідної інформації, яка становить конфіденційну, комерційну, або службову таємницю.

Також дії зовнішніх порушників можуть бути направлені на переманювання співробітників компанії.

Але найбільшу загрозу можуть представляти собою внутрішні порушники, так як вони мають доступ до інформації, який має статус КІ, або, наприклад, знали про

існуючі способи захисту даної інформації. Можна виділити 3 найпопулярніші причини внутрішнього порушника: безвідповідальність, самоствердження та з корисною метою.

- У разі безвідповідальних порушень користувач навмисно або випадково вчиняє деструктивні дії, не пов'язані зі зловмисним умислом. Зазвичай це наслідок некомпетентності або недбалості. Деякі користувачі сприймають доступ до системних записів як велике досягнення і грають у своєрідну гру «користувач проти системи», щоб заявити про себе чи інших співробітників компанії.
- Порушення безпеки АС може бути викликано власними інтересами користувача системи. У цьому випадку зловмисник спробує обійти систему безпеки, щоб отримати доступ до інформації АС. Навіть якщо автоматизована система має засоби, щоб зробити таке проникнення надзвичайно складним, повністю захистити її від проникнення практично неможливо. [18]

Отже, внутрішніми порушниками можуть бути як нечисті на руку керівники підприємств, рядові співробітники, до цієї категорії також відносяться і шахраї або аферисти.

Крім цього, необхідно звернути увагу на те, що співробітники можуть мати мотиви для нанесення шкоди для підприємства, якщо вони мають високий рівень самооцінки і можуть бути незадоволені або рівнем заробітної плати, або в них склалися погані відносини із колегами, або керівництвом підприємства.

Модель порушника має визначити:

- Категорія потенційних правопорушників.
- Рівень злочинних здібностей.
- Припущення про кримінальну кваліфікацію та можливі рівні знань.
- Методи та прийоми, що застосовуються при руйнуванні.
- Його градація за можливою метою порушника та ступеня небезпеки для АС.

- Можливі способи загрози з АС.
- Припущення про характер поведінки.

Категорії потенційних правопорушників:

Об'єкт розвідувальної діяльності - співробітники організації - власники АС (близько 81,7% збитків)

- внутрішній порушник.

Для визначення потрібні спеціальні можливості несанкціонованого доступу до ресурсів автоматизованої системи кожного співробітника в організації. Приблизно 17,3% шкоди завдають сторонні особи, які підтримують доступ до ресурсів АС)

- зовнішні порушники – при виявленні необхідно деталізувати основні можливості організації несанкціонованого доступу відвідувачів до ресурсів АС, а також систему організаційних обмежень доступу.

Порушників необхідно класифікувати за чотирма рівнями здібностей, залежно від кваліфікації, запропонованої персоналом AU. Класифікація є ієрархічною. Тобто наступний рівень функціональності включає можливу функціональність.

- Інформація 1 рівня про нижчий рівень можливості взаємодії з АС, можливість запуску набору фіксованих задач (програм), що реалізуються необхідними можливостями обробки.
- 2 рівень володіння створенням та запуском цих програм із новими можливостями обробки інформації.
- 3 рівень виробничого контролю операцій АС, тобто вплив на базове програмне забезпечення системи та налаштування та налаштування її обладнання.
- Інформація 4 рівня про повну функціональність особи, яка здійснює проектування, здійснює ремонт апаратних засобів АС, а також засобу, що підключає до АС, з використанням нових можливостей власної обробки.

Рівень порушника може бути висококваліфікованим спеціалістом (наприклад, адміністратором безпеки, бази даних, мережі) та може володіти повною інформацією про АС та комплекс засобів захисту. Враховуючи це порушників можна класифікувати за кваліфікацією та рівнем знань.

- Знати основні правила функціонування АС, формування масивів та потоку запитів до них, вміти користуватися штатними засобами обробки даних.
- Мати високий рівень та досвід роботи з технічними знаннями та системою її обслуговування.
- Мати передові знання в галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем.
- Знати структуру, функції, механізм захисту та їх сильні та слабкі сторони. [18]

Зрозуміло, що найнебезпечніші злочинці можуть знати:

1. Розташування, конфігурація, функціональні характеристики, режими та умови роботи елементів АС, включаючи маршрути можливих ліній зв'язку мережі зв'язку та трафік попутних каналів передачі даних.

2. Порядок, способи і режими роботи елементів АЕС, їх розташування (включаючи як точки, що обслуговуються, так і не обслуговуються) і прилеглі до них ділянки.

3. Організаційні процедури, засоби та режими - правові та технічні засоби захисту ресурсів.

4. Основні правила формування баз даних АС та подання заявок на них.

Залежно від методу і техніки, що використовується, його можна розділити на наступні категорії:

• Розвідувальні методи лише для отримання інформації.

• Пасивні технічні засоби перехоплення інформаційних сигналів.

• Недолік проектування CCIS для виконання лише співробітниками AU або спробами NSD.

• Зміни в методах та засобах, що позитивно впливають на АС, зміни в системі конфігурації (зміни штатних технічних засобів, підключення до каналів передачі даних, впровадження та використання спеціального програмного забезпечення тощо, або підключення додаткових засобів).

Ця класифікація порушників корисна в оцінці ризиків, аналізі вразливостей системи та ефективності різних запланованих процесів захисту.

Рис. 1.1. Класифікація загроз інформаційної системи

За місцем можливого порушення дії зловмисника поділяють на:

1. Немає доступу до зони управління (центральний рівень АС, регіональні рівні АС або робочі місця місцевих рівнів АС, пункти посилення служби) з технічними засобами дальньої розвідки (наприклад, оптичні канали, акустичні

канали, канали скремблування, електромагнітне випромінювання тощо) або шляхом отримання інформації з мережі передачі даних (наприклад, шляхом підключення чи «підключення» лінії зв'язку) – дистанційний вплив.

2. З доступом до контрольованої зони (центрального рівня ОС, регіональних рівнів ОС або термінальних робочих станцій, у тому числі віддалених користувачів ОС, пунктів підкріплення в сервісі, але без доступу до технічних засобів ОС) - також з використанням дистанційних розвідувальних оптичних, акустичних каналів, каналів електромагнітних перешкод тощо, з подальшим несанкціонованим доступом до будівель, споруд або приміщень, у яких виявляють елементи ОС (прямий вплив);

3. Доступ до робочих станцій кінцевих користувачів (включаючи віддалені робочі станції та сервіси, які не потребують технічного обслуговування) з наступним несанкціонованим доступом до пристроїв вводу-виводу, копіювальних пристроїв, каналів або канал утворюючих пристроїв та інших елементів ОС - прямий, як у 4 – 5 пунктах впливу;

4. Доступ до місць збору та зберігання даних (баз даних, архівів) з подальшим несанкціонованим тиражуванням фактичних носіїв даних, їх копій або інформації з таких накопичувачів і баз даних (наприклад, шляхом крадіжки, придбання тощо);

5. З доступом до засобів контролю та моніторингу інтегрованої системи ТЗІ з наступними майже необмеженими можливостями доступу до ресурсів автоматизованої системи, їх використання, зміни або знищення (крім того, що його дії фіксуються контролюючим органом системи ТЗІ) .

Вірогідною метою порушника може бути:

1. Персональна авторизація, а саме отримання персональних юридичних дозволів доступу, бажано з найбільш широкими правами, до ресурсів АС з метою їх використання, отримання необхідної інформації в необхідному обсязі та обсязі,

отримання конфіденційної інформації, зміна або знищення це відповідно до їхніх намірів (інтересів), планів);

2. Уповноваження своїх прихильників або довірених осіб, які могли б отримати юридичні атрибути доступу, бажано з найбільшими правами, до ресурсів АС для їх використання, отримання необхідної інформації в необхідному обсязі та обсязі, доступу до конфіденційної інформації, модифікації або знищення, відповідно до до своїх інтересів;

3. Шукати прихильників або довірених осіб серед співробітників або користувачів АС, яким надано атрибути легального доступу, бажано з найбільшими правами на ресурси АС, і можуть їх використовувати – бажано отримувати, редагувати або знищувати конфіденційну інформацію; у разі відсутності у правопорушника здатності або невиконання пунктів 1 - 3 зловмисник може спробувати:

4. Отримання атрибутів доступу авторизованих користувачів за допомогою технічних засобів, покупки, крадіжки чи іншим чином;

5. Проникнення будь-якого елемента, компонента або ресурсу АС (інформаційні ресурси, обчислювальні ресурси, прикладне, базове програмне забезпечення та системне програмне забезпечення ТСІ, включаючи резервні носії, телекомунікаційне обладнання, включаючи мережу даних, ресурси вводу-виводу) шляхом подолання перешкод, огорож, компонентів охоронних систем або систем охоронної сигналізації тощо, а також пошкодження, спричинені знищенням інформації, майна;

6. Зміна функціонування або виведення з експлуатації матеріальних ресурсів АС;

7. Встановлення фізичних засобів (апаратних закладок) або інших засобів технічної розвідки в місцях розташування елементів АС (у тому числі віддалених елементів, наприклад, в елементах мережі зв'язку) для збору інформації;

8. Встановлення фізичних або інших засобів (апаратних закладок) у місцях розташування елементів АС (у тому числі віддалених елементів, наприклад, в елементах мережі зв'язку) для створення неправдивих сигналів, інформаційних символів або повідомлень;

9. Налаштування програмних засобів (програмних закладок) для збору інформації для використання від свого імені;

10. Встановлення програмного забезпечення (закладок програмного забезпечення або вірусів) для модифікації як програмного забезпечення, так і інформації АС шляхом генерації (впровадження) програмних вірусів, помилкових тривог, інформаційних піктограм або повідомлень, щоб перевантажити системи АС і таким чином забезпечити доступність компонентів АС або динамка порушувати ціле;

11. Спроба несанкціонованого доступу до комп'ютерів, інформаційних ресурсів, основного та прикладного програмного забезпечення та програмного забезпечення системи TSI як самої АС та її телекомунікаційної підсистеми шляхом порушення системи контролю доступу.

Залежно від характеру зловмисника, він може становити активну або пасивну загрозу ресурсам автоматизованої системи.

Активні загрози означають спроби навмисної несанкціонованої зміни стану АС, а пасивні загрози – спроба несанкціонованого проникнення в систему без зміни її стану. Відповідно за характером дій порушників можна класифікувати на:

- «випадкові порушники» – авторизовані користувачі, які порушили політику безпеки підприємства не навмисно, а випадково – внаслідок випадкового подолання засобів контролю (адміністрування) шляхом доступу до об'єкта, що охороняється, вчинення непередбачених дій щодо цього об'єкта тощо;
- «терплячі порушники» — авторизовані користувачі, які навмисно, але без рішучих дій порушили політику безпеки певного сервісу, маскуючись шляхом вибору атрибутів доступу інших користувачів для прихованого подолання засобів контролю (керування) доступом до нього тощо;
- «рішучі порушники», - порушники мають ціль в будь-якому випадку порушити ту чи іншу властивість захищеної інформації; для цього типу правопорушника притаманне подолання засобів організаційного доступу до

будівель, доступу до фізичних ресурсів, конструктивних елементів, систем виявлення вторгнень тощо;

- правопорушники, що використовують спеціальне обладнання, засоби доступу до інформаційних об'єктів: витік технічних каналів, особливий вплив на інформацію по технічним каналам, мережі локальних або розподілених мереж, що входять до складу засобів телекомунікаційних мереж.

Також слід зазначити, що порушення з боку цих осіб можуть бути як зловмисними, так і ненавмисними. Найбільшої небезпеки зазвичай очікують зловмисних порушників. *Ненавмисний зловмисник* може створити випадкові загрози ресурсам автоматизованої системи при виконанні її функціональних обов'язків в результаті помилкових дій через неуважність або недбалість.

Давайте з'ясуємо, які з можливих способів використання загроз в АС:

- технічними каналами, які включають канали побічних електромагнітних випромінювань і наводок, акустичні, вібро-акустичні, акусто-електричні, оптичні, радіо- та радіотехнічні, хімічні канали тощо;
- канали із спеціальним впливом шляхом створення полів і сигналів для порушення цілісності інформації або навіть руйнування системи захисту;
- несанкціонований доступ шляхом підключення до пристроїв і ліній зв'язку, порушення заходів безпеки з метою використання інформації або нав'язування неправдивої інформації, маскування під зареєстрованого користувача, використання вбудованих пристроїв або програм, а також коріння комп'ютерних вірусів. [7, 17]

1.3. Огляд існуючих моделей порушника

Відповідно до НД ТЗІ 1.1-001-99 «Технічний захист інформації на програмно-керованих АС загального користування» ми можемо побачити, що для систем розглядаються три групи моделей порушників.

1. Перша група показує порушників, які реалізують загрози на одній підсистемі з боку іншої підсистеми.

2. Друга містить у собі моделі порушників, які реалізують загрози на підсистемі керування.

3. Третя - порушники, які реалізують загрози на підсистемі зв’язку.

Розглянемо їх докладніше [4]:

Таблиця. 1.1.

Перша група моделі порушника

Код моделі порушника	Найменування моделі порушника	Рівні можливостей порушників
МН 1.01	Модель порушника ПРД до інформаційних ресурсів підсистеми керування станцією	Порушник намагається порушити встановлені ПРД до ресурсів підсистеми керування АС з боку підсистеми зв’язку. Порушник має один рівень навичок - можливість вибрати прикладну задачу і вести діалог у її середовищі, наприклад, запуск завдань (програм) з фіксованого набору, що реалізують встановлені функції (сервіси) для обробки інформації; діалог під час запуску активних завдань; Реконфігурація термінального обладнання та послуг, що надаються засобами програмне забезпечення
МН 1.02	Модель порушника, який використовує помилки або некоректні дії суб’єктів, що допущені на будь-якій із фаз життєвого циклу АС, для реалізації загроз на підсистемі управління	Розрізняють порушника - джерела помилок або неправильних дій і порушника - реалізатора загроз інформації в підсистемі управління станцією, що працює з боку підсистеми зв’язку. Передбачається, що зловмисник - джерело помилок або неправильних дій, може мати статус авторизованого користувача з будь-яким допустимим рівнем повноважень і може мати доступ до будь-яких звичайних механізмів взаємодії авторизованого користувача із середовищем для розробки, виготовлення та/або експлуатації АС на будь-якому етапі його життєвого циклу.

Продовження табл. 1.1

	шляхом впливу на інформацію з боку підсистеми зв’язку	Порушник також може бути зі статусом авторизованого користувача з будь-яким допустимим рівнем повноважень, але діє лише на етапі промислової експлуатації АС
МН 1.03	Модель зловмисника, що користується програмним забезпеченням та/або технічними пристроями, встановленими у підсистемі керування АС, шляхом їх активації за спеціальними каналами	Порушники можуть бути установниками технічних пристроїв та (або) самостійними установники програмного забезпечення АС та підсистема контролю вторгнень, що працює від підсистеми зв'язку. Передбачається, що порушник - установник незалежних пристроїв матиме статус авторизованого користувача з будь-яким допустимим рівнем повноважень та мати доступ до середовища розробки, виготовлення та/або експлуатації підсистеми керування АС на будь-якому етапі свого життєвого циклу. Зловмисник також може мати статус авторизованого користувача з будь-яким авторизованим рівнем повноважень, але діє лише на етапі промислової експлуатації АС
МН 1.04	Модель порушника, що користується позаштатними програмно-апаратними пристроями, встановленими на підсистемі зв'язку, шляхом їхньої активізації через спеціальні канали впливу з боку підсистеми керування	Розрізняють порушника – установника позаштатних програмно-апаратних пристроїв на підсистемі зв’язку і порушника – реалізатора загроз для інформації, який діє з боку підсистеми керування станцією. Передбачається, що установник-порушник може мати статус авторизованого користувача з будь-яким допустимим рівнем повноважень та мати доступ до середовища розробки, виготовлення та/або експлуатації підсистеми зв'язку АС на будь-якому етапі її життєвого циклу. Розробник-порушник також може мати статус авторизованого користувача з будь-яким дозволеним рівнем повноважень, але діє лише на етапі промислової експлуатації АС

Продовження табл. 1.1

МН 1.05	Модель порушника, яка використовує якісну неадекватність інформаційно-вразливих режимів, функцій і послуг, що надаються АС, для реалізації загроз підсистемі зв'язку через підсистему управління	Розрізняють зловмисника - джерела якісної неадекватності режимів, функцій або послуг і зловмисника - реалізатора загроз на підсистему зв'язку, що діє з підсистеми управління станцією. Здібності злочинця надаються відповідно до моделі МН 1.04.

Таблиця 1.2.

Друга група моделі порушника

Код моделі порушника	Найменування моделі порушника	Рівні можливостей порушників
МН 2.01	Модель порушника ПРД	Передбачається, що зловмисник намагатиметься зламати діючі ПРД , використовуючи звичайну службу обслуговування АС. У цьому випадку рівень навичок порушника моделі МН 2.01 відповідає рівню навичок порушника моделі МН 1.01.
МН 2.02	доступу) на елементи підсистеми управління АС	Передбачається, що порушник має дозвіл на доступ. Програмне забезпечення та/або до апаратних елементів підсистеми управління ОС.

Продовження табл. 1.2

МН 2.03	Модель порушника, реалізуючий недопустимі впливи на параметри середовища експлуатації АС з цілю порушення доступу до підсистеми керування	Передбачається, що порушник намагається спричинити збої або вихід з ладу АС через параметри середовища, в якому працює система управління станції, що виходять за межі нормальних значень (наприклад, через навмисний вплив з боку електромережі, радіоактивне або теплове випромінювання, елементи обладнання, порушення в роботі електрики чи кондиціонування тощо). Розглядаються два рівні порушника: перший - якщо порушник знаходиться в межах контрольованої зони і має право доступу до станційного обладнання ОС; другий - якщо порушник знаходиться за межами контрольованої зони.
МН 2.04	Модель порушника, що впливає позаштатними засобами на елементи підсистеми керування АС	Вважається, що порушник має право доступу до програмного та/або апаратного забезпечення підсистеми управління ОС.
МН 2.06	Модель порушника через канали ПЕМВН	Порушник прагне порушити конфіденційність інформації сучасними засобами прийому та розподілу інформативні параметри ПЕМВН, що формуються за елементами підсистеми керування АС, управляє підсистемами чи відвідуваннями кінцевих ліній за рахунок ПЕМВН із зовнішніх джерел. Розглядаються два рівні можливостей Порушник перший – якщо порушник знаходиться у контрольованій зоні об'єкта станції АС; другий - коди порушник перебуває поза контрольованою зоною

Продовження табл. 1.2

МН 2.07	Модель порушника через канали побічних акусто-електричних перетворень на терміналах обслуговування АС	Підозрюється, що порушник намагається порушити конфіденційність інформації, має сучасні засоби розподілу доходу та посилення інформаційних сигналів, які можуть з'являтися на лініях кінцевого обладнання внаслідок непрямих акустико-електричних перетворень інформаційних сигналів у кінцевому обладнанні підсистеми керування гучномовцем. При цьому враховується один рівень можливостей зловмисника - якщо порушник має право доступу до термінальних ліній у контрольованій зоні обладнання станції АС
МН 2.08	Модель порушника, використовуючого помилки або некоректність дій суб'єктів доступу до підсистеми керування або її документації, що допущені на передексплуатаційному етапі життєвого циклу АС	Вважається, що порушники як джерело помилок та/або некоректних дій, так і реалізатор загроз для інформації діють на підсистемі керування АС і мають компетенції для доступу до програмного забезпечення та/або до елементів устаткування АС
МН 2.09	Модель порушника, використовуючого помилки або некоректні дії персоналу АС при зберіганні критичної інформації на фізичних носіях	Передбачається, що порушники можуть бути уповноваженими для доступу до критичної інформації на фізичних носіях.

Продовження табл. 1.2

МН 2.10	Модель порушника, використовуючого випадкові збої і відмови в роботі підсистеми керування АС	Передбачаються можливості персоналу АС.

Таблиця 1.3.

Третя група моделі порушника

Код моделі порушника	Найменування моделі порушника	Рівні можливостей порушників
МН 3.01	Модель порушника, який реалізує неприпустимі впливи через штатні засоби станції на елементи підсистеми зв'язку АС	Розглядаються два рівні можливостей порушника: перший — коли зловмисник має право доступу до елементів підсистеми зв'язку; другий - якщо зловмисник не має дозволу на доступ до елементів обладнання підсистеми зв'язку. Вважається, що порушник намагається маніпулювати елементи обладнання підсистеми зв'язку, що змінює функції, які виконує станція або послуги, що надаються користувачу, та має сучасне обладнання підсистеми зв'язку, впливу на програмне та апаратне забезпечення АС.
МН 3.02	Модель порушника, що чинить неприйнятний вплив на параметри середовища експлуатації АС	Передбачається, що зловмисник намагається викликати збої або помилки в роботі АС шляхом виведення параметрів зовнішнього середовища, в якому функціонує комунікаційна підсистема, за межі стандартних значень. При цьому враховуються два рівні можливостей зловмисника: перший – якщо зловмисник має дозвіл доступу до обладнання підсистеми зв'язку;

Продовження табл. 1.3

	для порушення працездатності елементів підсистеми зв'язку	другий - якщо правопорушник не має такої можливості
МН 3.03	Модель порушника, що чинить вплив позаштатними засобами на елементи підсистеми зв’язку АС	Вважається, що порушник намагатиметься реалізувати інформаційну загрозу за допомогою сучасних позаштатних засобів впливу, у тому числі засобів видалення інформації з цифрових та аналогових абонентських ліній та між станцій. З цього випливають два рівні можливостей порушника: перший - коли порушник має право доступу до елементів підсистеми комунікацій; другий – коли порушник не має таких повноважень
МН 3.04	Модель порушника, використовуючий програмні закладки та/або апаратні закладні пристрої, що встановлені на підсистемі зв’язку АС	Порушник (наприклад, установники вбудованих пристроїв, та розробники інформаційних загроз) працюють над підсистемою зв’язку, і їх рівень кваліфікації відповідає рівню навичок для моделі МН 2.05.
МН 3.05	Модель порушника через канали ПЕМВН	Передбачається, що порушник намагатиметься зламати конфіденційність інформації, наявність сучасних засобів прийому та присвоєння інформаційних параметрів, що формуються ПЕМВН елементи устаткування ліній зв'язку, чи відвідування лінії зв'язку з допомогою ПЕМВН із зовнішніх джерел інформації. При цьому враховуються два рівні можливостей злочинця: перший – коли порушник перебуває у контрольованих зонах; другий – коли порушник перебуває поза контрольованими зонами.

Продовження табл. 1.3

МН 3.06	Модель порушника, використовуючого помилки або некоректні дії суб'єктів доступу до підсистеми зв'язку або її документації, що допущені на передексплуатацій них стадіях життєвого циклу АС	Порушники вважаються, як джерело помилки або невірних дій та виконавці інформаційної загрози, діють на підсистему комунікацій і їхні рівні кваліфікації відповідають рівням кваліфікації зловмисника для моделі МН 1.02.
МН 3.07	Модель порушника, використовуючого непередбачувані збої і відмови в роботі елементів підсистеми зв'язку АС	Передбачаються можливості персоналу АС

Розглянемо основні критерії моделей порушника, які були надані вище:

- Можливість порушення ПРД
- Отримання статусу авторизованого користувача
- Використання помилок або некоректних дій суб'єктів, збоїв або відмови в роботі АС
- Використання програмних позаштатних пристроїв
- Використання програмно-технічні позаштатні пристроїв
- Використання недостатності якості функцій і послуг, інформаційно-уразливих режимів, що надаються АС, та можливе виведення з робочого стану
- Порушення доступності до підсистеми керування
- Використання канал побічних електромагнітних випромінювань

Таблиця 1.4.

Порівняння моделей порушників за критеріями

Модель порушника / Критерій	Можливість порушення ПРД	Отримання статусу авторизованого користувача	Використання помилок або некоректних дій суб'єктів, збоїв або відмови в роботі АС	Використання програмних позаштатних пристроїв	Використання програмно-технічні позаштатні пристроїв	Використання недостатності якості інформаційно-уразливих режимів, функцій і послуг, що надаються АС, та можливе виведення з	Використання канал побічних електромагнітних випромінювань
МН 1.01							
МН 1.02							
МН 1.03							
МН 1.04							
МН 1.05							
МН 2.01							
МН 2.02							
МН 2.03							
МН 2.04							
МН 2.05							
МН 2.06							
МН 2.07							
МН 2.08							
МН 2.09							
МН 2.10							
МН 3.01							
МН 3.02							
МН 3.03							
МН 3.04							
МН 3.05							
МН 3.06							
МН 3.07							
МН 3.08							

1.4. Аналіз автоматизованих систем побудови різноманітних моделей

Процеси моделювання все більше виконуються з використанням спеціального програмного забезпечення для автоматизації цієї діяльності.

Автоматизована система моделювання або автоматизована система моделювання (АСМ) - комп'ютерна система, призначена для допомоги користувачеві у поданні шуканої задачі у вигляді прийнятої в цій системі

математичної схеми, вирішенні задачі (моделюванні отриманої схеми) та аналізі результатів.

До засобів та засобів автоматизованого проектування та розробки інформаційних систем належать CASE-інструменти та системи, призначені для підтримки розробки інформаційних систем.[23]

Програмне забезпечення моделювання інформаційних ризиків часто використовується для створення моделі системи та виявлення вразливостей. Найпоширенішими програмами такого типу є [25]:

- Microsoft Threat Modeling Tool – безкоштовна програма, розроблена компанією Microsoft для методології STRIDE, дозволяє створити блок-схему, діаграму в системі та створити детальний звіт у форматі HTML про всі можливі вразливості у вашій системі. Ось деякі інструменти та інновації:
  - Автоматизація: Керівництво та зворотній зв'язок у кресленні моделі
  - STIDE per Element: керований аналіз загроз та їх пом'якшення
  - Звітування: заходи безпеки та тестування на етапі верифікації
  - Унікальна методологія: дозволяє користувачам краще візуалізувати та розуміти загрози
  - Розроблено для розробників і зосереджено на програмному забезпеченні: багато підходів зосереджені на активах або зловмисниках. Зосереджено на програмному забезпеченні. Спирається на дії, з якими знайомі всі розробники та архітектори програмного забезпечення, наприклад малювання зображень для архітектури програмного забезпечення. [26]
- Mozilla threat modeling tool – безкоштовний онлайн застосунок, розроблений Mozilla для моделювання інформаційних ризиків;
- OWASP Threat Dragon - безкоштовне програмне забезпечення для моделювання онлайн-загроз із відкритим кодом із системними діаграмами та механізмом автоматичного генерування загроз. Для моделювання загроз з відкритим кодом для команд впроваджують підхід STRIDE. Його також

можна використовувати для класифікації загроз за допомогою LINDDUN і CIA. Основними напрямками інструменту є:

- Чудовий UX – використання Threat Dragon має бути простим, захоплюючим і веселим
- Потужний механізм правил загрози/пом'якшення – це знижує бар'єр для входу для команд і дозволяє нефахівцям робити свій внесок
- Точки інтеграції з іншими інструментами життєвого циклу розробки - коли це буде впроваджено, це гарантує, що моделі легко включаються в життєвий цикл розробки та залишаться актуальними в міру розвитку проекту. [27]

- MyAppSecurity пропонує перший комерційно доступний інструмент моделювання загроз – ThreatModeler. В ньому використовується методологія VAST, заснований на PFD і визначає загрози на основі великої бібліотеки загроз. Дає можливість корпоративним IT-організаціям відображати свої унікальні вимоги та політики безпеки безпосередньо в кіберсистемі підприємства, забезпечуючи в режимі реального часу ситуаційну обізнаність про їхній портфель загроз та умови ризиків.[28]
- IriusRisk — надає персональні та комерційні версії програми. Ця програма орієнтована на створення та підтримку моделі загроз у реальному часі. Вона керує процесом за допомогою анкет і бібліотек, моделей ризиків, що повністю настроюються, а також об'єднує кілька інших інструментів (OWASP ZAP, BDD-Security, Threadfix...) для поліпшення автоматизації процесу моделювання ризиків.
- securiCAD — інструмент моделювання загроз та управління ризиками, розроблений скандинавською компанією Providet. Створено CISO для управління корпоративною кібербезпекою для інженерів з безпеки та технічного персоналу. SecuriCAD виконує автоматизоване моделювання атак для поточних та майбутніх інформаційних архітектур, всебічно ідентифікує та кількісно оцінює ризики, пов'язані зі структурними

вразливістю, та забезпечує підтримку прийняття рішень на основі результатів. Ключові переваги:

- Цілісний - цілісна оцінку ризиків архітектури та дослідження, яку комбінацію вразливостей зловмисник може використати, щоб отримати доступ до цінних активів
- Проактивний - вивчення ризиків змодельованих атак до того, як вони відбудуться, і оцініть нові проекти перед розгортанням
- Автоматизований - автоматична генерація моделі своєї архітектури та запускайте повністю автоматизоване моделювання атак на моделі
- Незривний - моделювання атак проводиться на моделях архітектури і ніколи не впливає на реальне середовище. [29]

• SD Elements by Security Compass — платформа керування вимогами безпеки до програмного забезпечення, включає можливості автоматизованого моделювання вразливостей. Серія загроз створюється шляхом заповнення короткої анкети про технічні деталі програми та драйвери. Контрзаходи представлені як завдання, які розробники повинні виконати для створення захисту. SD Elements не тільки допомагає командам вбудовувати безпеку в свої програми та керувати вимогами безпеки в SDLC, але й створює перевірений запис усіх дій. Нові та суворі закони про кібербезпеку, такі як GDPR та NY DFS, вимагають від компаній не лише дотримуватися безпечних процедур розробки, але й мати можливість доводити відповідність регулюючим органам. SD Elements робить це, а корпоративну підзвітність легко. Якщо компанія зазнала зламу даних, CIO та CISO можуть довести, що компанія дотримується належної політики безпеки додатків, або, навпаки, визначити, що і хто був відповідальним за порушення. [30]

Таблиця 1.5.

Порівняння автоматизованих систем побудови моделей по критеріям

Критерій / Програма	Microsoft threat modeling tool	Mozilla threat modeling tool	OWASP Threat Dragon	Threat Modeler	IriusRisk	securiCAD	SD Elements by Security Compass
Безкоштовне використання	+	+	+	-	-	-	-
Український інтерфейс	-	-	-	-	-	-	-
Зручний, сучасний дизайн	+	-	+	-	+	+	+
Створення моделі за допомогою анкетування	-	-	-	-	-	-	+
Можливість редагування	+	-	+	+	+	+	+
Виведення результатів в таблиці	-	+	-	-	-	-	-
Створення діаграм/графіків	+	-	+	+	+	+	+
Можливість створення моделі порушника	-	-	-	-	-	-	-

1.5. Висновки до розділу

В першому розділі було розглянуто автоматизовані системи побудови моделей, модель порушника, види його моделей. В розділі описуються можливості порушника, його ймовірні дії і принципи роботи, мета дій. Було проаналізовано існуючи моделі порушника для автоматизованих систем, порівняно їх по критеріям, а також автоматизовані системи побудови систем.

Відповідно до дослідження можна сказати, що модель порушника грає велику роль за інформаційної безпеки підприємств. Невірно побудована модель порушника може мати негативні наслідки при настанні інцидентів інформаційної безпеки, що приведе як до матеріальних втрат, так і до втрати іміджу, довіри компанії, що знову приведе до матеріальних втрат.

Проаналізувавши порівняння моделей порушників і різні автоматизовані системи побудови моделей, а також ознайомившись з методами створення моделі порушника, можна розробляти автоматизовану систему побудови моделі порушника.

РОЗДІЛ 2
РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ПОБУДОВИ МОДЕЛІ ПОРУШНИКА

2.1. Розробка питань для побудови можливих порушників

На даний час, не існує затвердженої методики для побудови моделі порушника та моделі загроз.

Правильність розробки моделі порушника являється гарантією побудови адекватної системи забезпечення інформаційної безпеки. Грунтуючись на побудовану модель, можна створити адекватну систему інформаційного захисту.

Зазвичай створюється неформальна модель порушника, яка відображає причини та мотиви дій, його навички, апріорні знання, цілі та їх пріоритетність для порушника, основні шляхи досягнення цілей: способи, місця та види дій, діяльність, можлива тактика тощо. Для того, щоб дійти до цілі, зловмиснику необхідно докласти зусиль і витратити ресурси. [24]

Для формування моделі можемо сформулювати такі питання (рис 2.1, 2.2):

1. Скільки приміщень має підприємство?
2. Яка кількість ПК на підприємстві?
3. Чи організовано на підприємстві закріплення ОПК за кожним співробітником?
4. Чи організовано на підприємстві розмежування інформації між її співробітниками?
5. Чи можливий доступ сторонніх до приміщень підприємства?

Для визначення, яка інформація з обмеженим доступом використовується на підприємстві допоможуть такі питання (6-8):

6. Конфіденційна інформація?
7. Службова інформація?
8. Таємна інформація?

9. Яка секретність інформації з обмеженим доступом на підприємстві з огляду на можливі наслідки з її розповсюдженням?
10. Яка цінність інформації для функціонування підприємства?
11. Чи організовано на підприємстві періодична перевірка функціонування АС та її захисту?
12. Яка періодичність перевірок на рік?
13. Чи проводиться на підприємстві навчання Політики безпеки інформації?
14. Чи проводиться на підприємстві перевірка знань Політики безпеки інформації?
15. Яка періодичність перевірок на рік? Написати цифру.
16. Чи сформовано відділ інформаційної безпеки на підприємстві?
17. Чи прописані процедури та заходи реагування на інциденти порушення безперервної діяльності компанії? Чи ознайомлений персонал з цією інформацією?
18. Які можливі втрати від ймовірного порушення безперервної діяльності компанії?
19. Чи сформовано Інструкцію з організації парольного захисту?
20. Чи заборонені на підприємстві особисті зовнішні носії?

Чи організовано на підприємстві розмежування інформації між її співробітниками? Якщо ТАК	0,1
Чи можливий доступ сторонніх до приміщень підприємства? Якщо ТАК - 1, НІ - 0	0,1
Необхідно вказати, яка інформація з обмеженим доступом використовується на підприємстві? Конфіденційна інформація. Якщо ТАК - 1, НІ - 0	0,1
Службова інформація. Якщо ТАК - 1, НІ - 0	0,1
Таємна інформація. Якщо ТАК - 1, НІ - 0	0,1
Яка секретність інформації з обмеженим доступом на підприємстві з огляду на можливі наслідки з її розповсюдженням? Без наслідків - 1, Низька - 2, Середня - 3, Висока - 4, Дуже висока - 5	Any
Яка цінність інформації для функціонування підприємства? Низька - 1, Середня - 2, Висока - 3, Дуже висока - 4	Any
Чи організовано на підприємстві періодична перевірка функціонування АС та її захисту? Якщо ТАК - 0, НІ - 1	0,1
Яка періодичність перевірок на рік? Написати цифру	Any
Чи проводиться на підприємстві навчання Політики безпеки інформації? Якщо ТАК - 0, НІ - 1	0,1
Чи проводиться на підприємстві перевірка знань Політики безпеки інформації? Якщо ТАК - 0, НІ - 1	0,1
Яка періодичність перевірок на рік? Написати цифру	Any
Чи прописані процедури та заходи реагування на інциденти порушення безперервної діяльності компанії? Чи ознайомленний персонал з цією інформацією? Якщо ТАК - 0, НІ - 1	0,1
Які можливі втрати від ймовірного порушення безперервної діяльності компанії? Низькі - 1, Середні - 2, Високі - 3, Дуже високі - 4	Any
Чи заборонені на підприємстві особисті зовнішні носії? Якщо ТАК - 0, НІ - 1	0,1
Чи сформовано Інструкцію з організації парольного захисту? Якщо ТАК - 0, НІ - 1	0,1

Рис. 2.1 Питання та можливі відповіді для побудови моделі порушника для АС 1 класу

Скільки приміщень має підприємство? Написати цифру	Any
Яка кількість ПК на підприємтсві? Написати цифру	Any
Чи організовано на підприємстві закріплення ПК за кожним співробітником? Якщо ТАК - 0, НІ - 1	0,1
Чи організовано на підприємстві розмежування інформації між її співробітниками? Якщо ТАК - 0, НІ - 1	0,1
Чи можливий доступ сторонніх до приміщень підприємства? Якщо ТАК - 1, НІ - 0	0,1
Необхідно вказати, яка інформація з обмеженим доступом використовується на підприємстві? Конфіденційна інформація. Якщо ТАК - 1, НІ - 0	0,1
Службова інформація. Якщо ТАК - 1, НІ - 0	0,1
Таємна інформація. Якщо ТАК - 1, НІ - 0	0,1
Яка секретність інформації з обмеженим доступом на підприємстві з огляду на можливі наслідки з її розповсюдженням? Без наслідків - 1, Низька - 2, Середня - 3, Висока - 4, Дуже висока - 5	Any
Яка цінність інформації для функціонування підприємства? Низька - 1, Середня - 2, Висока - 3, Дуже висока - 4	Any
Чи організовано на підприємстві періодична перевірка функціонування АС та її захисту? Якщо ТАК - 0, НІ - 1	0,1
Яка періодичність перевірок на рік? Написати цифру	Any
Чи проводиться на підприємстві навчання Політики безпеки інформації? Якщо ТАК - 0, НІ - 1	0,1
Чи проводиться на підприємстві перевірка знань Політики безпеки інформації? Якщо ТАК - 0, НІ - 1	0,1
Яка періодичність перевірок на рік? Написати цифру	Any
Чи сформовано відділ інформаційної безпеки на підприємстві? Якщо ТАК - 0, НІ - 1	0,1
Чи прописані процедури та заходи реагування на інциденти порушення безперервної діяльності компанії? Чи ознайомленний персонал з цією інформацією? Якщо ТАК - 0, НІ - 1	0,1
Які можливі втрати від ймовірного порушення безперервної діяльності компанії? Низькі - 1, Середні - 2, Високі - 3, Дуже високі - 4	Any
Чи сформовано Інструкцію з організації парольного захисту? Якщо ТАК - 0, НІ - 1	0,1
Чи заборонені на підприємстві особисті зовнішні носії? Якщо ТАК - 0, НІ - 1	0,1

Рис. 2.2 Питання та можливі відповіді для побудови моделі порушника для АС 2, 3 класів

Згідно цим питанням зацікавлені юридичні особи зможуть отримати модель порушника для свого підприємства, не зважаючи, яка на підприємстві автоматизована система – першого, другого або третього класу. Для кожного класу автоматизованої системи підібрані саме ті питання, завдяки яким можна побудувати модель порушника, яка буде одним з основних складників при побудові системи інформаційної безпеки цим підприємством.

На кожне питання буде запропоновано від 1 до 5 варіантів відповідей. Особа, яка буде надавати відповіді має вносити їх точно, відповідно до уточнень після кожного питання.

Усі відповіді будуть вноситися в файл Excel, і підприємство матиме можливість перевірити правильність вводу інформації, коли в цьому буде необхідність.

2.2. Можливі порушники для побудови моделі порушника

Побудова моделі порушника буде відбуватися відповідно до опитувальнику, наданому в пункті 2.1.

Приблизний список можливих порушників, а також їх можливості надані в табл. 2.1. Цей список може змінюватися при необхідності для кожної компанії. Для кожного підприємства рекомендовано змінювати, або додавати посади робітників, відповідно до робочого складу компанії для побудови якнайбільш точної моделі внутрішнього порушника, який може бути найбільш небезпечний для деяких підприємств.

Таблиця 2.1.

Можливі порушники і їх можливості

№	Назва порушника	Узагальнені можливості порушника
	Зовнішній порушник	
1	Спеціальні служби іноземних держав	Здатність самостійно розробляти методи атаки, готувати та проводити атаки на контрольований доступ до обладнання з фізичним доступом; Залучення спеціалістів з досвідом розробки та аналізу інтегрованих систем інформаційної безпеки (в т.ч. спеціалістів у галузі аналізу лінійних сигналів передачі та компромісу електромагнітного випромінювання та індукції)
2	Терористичні, екстремістські угруповання	Здатність самостійно розробляти методи атаки, готувати та виконувати атаки за межами контрольованої зони та в межах контрольованої зони, але без фізичного доступу до обладнання.
3	Злочинні групи (кримінальні структури)	Можливість самостійно розробляти методи атаки, готувати та виконувати атаки тільки за межами контрольованої зони
4	Конкуруючі організації	Здатність самостійно створювати методи атаки та поведінку всередині та поза контрольованою зоною, але без фізичного доступу до обладнання.
5	Розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів	Можливість впроваджувати додаткові функції в ПЗ або і програмне, і апаратне забезпечення під час розробки.
6	Зовнішні суб'єкти (фізичні особи)	Можуть мати інформацію про вразливості в інформаційних системах, опублікованих у відкритих джерелах. Можливість самостійно створювати методи атаки, готувати та виконувати атаки тільки за межами контрольованої зони

Продовження табл. 2.1

7	Колишні працівники	Знають інформаційну структуру та порядок захисту інформаційних ресурсів в організації Здатність самостійно здійснювати створення методів нападу, підготовку та проведення атак лише за межами контрольованої зони
8	Клієнти	Здатність самостійно створювати методи атаки, готувати та проводити атаки за межами контрольованої зони та всередині контрольованої зони, але без фізичного доступу до обладнання
	Внутрішній порушник	
9	Директор	Повний доступ до інформаційної системи
10	Бухгалтер	Повний доступ до фінансових документів, Доступ до комп'ютерів більшості працівників
11	Юрист	Повний доступ до юридичної документації та архіву компанії
12	IT-спеціаліст	Повний доступ до інформаційної системи Можливість внесення змін в інформаційній системі без вірогідного виявлення іншими співробітниками
13	Прибиральник	Доступ до різних приміщень і кожного робочого місця персоналу, в тому числі і керівництва компанії Доступ до комп'ютерів мінімізований
14	Охоронник	Постійний візуальний доступ, а також фізичний доступ до різних приміщень і кожного робочого місця персоналу, в тому числі і керівництва компанії Доступ до комп'ютерів мінімізований

З табл. 2.1 можна побачити, що найбільші втрати можна отримати від зовнішнього порушника, адже він має більше можливостей і більший функціонал. Зазвичай зовнішні порушники мають знання та навички, завдяки яким порушення некоректно працюючої інформаційної безпеки підприємства може завдати великих втрат для компанії

Внутрішній порушник, зазвичай, може порушити інформаційну безпеку випадково, через халатне відношення до правил безпеки, також мотивацією

внутрішнього порушника, як правило, не вищого керівництва компанії, може бути маніпулювання зовнішніми особами, нелояльне відношення до компанії/співробітників/керівництва, або ж образа на них.

Для визначення мотивації зовнішнього порушника сформуємо табл. 2.2.

Таблиця 2.2.

Можливі зовніші порушники і їх мотивація

№	Назва порушника	Мотивація порушника
1	Спеціальні служби іноземних держав	Завдання збитків державі; Отримання інформації з обмеженим доступом з подальшим використанням в своїх цілях
2	Терористичні, екстремістські угруповання	Завдати шкоди державі, окремим сферам її діяльності чи галузям економіки. Вчиняє терористичні акти. Політична чи ідеологічна мотивація
3	Злочинні групи (кримінальні структури)	Отримання інформації з обмеженим доступом з подальшим використанням для злочинних дій (шантаж, дискредитація тощо)
4	Конкуруючі організації	Дискредитація компанії, для покращення положення на ринку
5	Розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів	Завдання майнової шкоди в разі шахрайства або зловживання довірою. Необережні, випадкові чи некваліфіковані дії
6	Зовнішні суб'єкти (фізичні особи)	Виявлення вразливостей з метою їх подальшого продажу і отримання фінансової вигоди
7	Колишні працівники	Дискредитація компанії як наслідок образи або нелояльного відношення до компанії/керівництва/співробітників. Отримання інформації з обмеженим доступом для подальшого продажу.

Продовження табл. 2.2

8	Клієнти	Дискредитація компанії як наслідок образи або нелояльного відношення до компанії/керівництва/співробітників. Отримання інформації з обмеженим доступом для подальшого продажу

Таблиця 2.3.

Оцінка потенціалу/ймовірності порушника

Отриманий результат дослідження	Потенціал/ймовірність порушника
0-5	найнижчий
5-10	низький
10-20	середній
20-	високий

2.3. Створення автоматизованої системи побудови моделі порушника

2.3.1. Використане програмне забезпечення

1. Microsoft Visual Studio — лінійка продуктів компанії Microsoft, куди входить інтегроване середовище розробки програмного забезпечення та інші інструменти. Дана продукція дозволяє розробляти як консольні програми, так і ігри та програми з графічним інтерфейсом, у тому числі з підтримкою технології Windows Forms, UWP а також веб-служби, веб-програми, веб-сайти, як в рідному, так і в керованому кодах всіх платформ, підтримуваних Windows, Windows CE, Windows Mobile, Windows Phone, .NET Framework, Compact Framework, .NET Core, .NET, MAUI, Xbox,.NET та Silverlight. Після придбання компанії Xamarin корпорацією Microsoft з'явилася можливість розробки IOS та Android програм.

Visual Studio складається з редактору вихідного коду з технологією IntelliSense і простим перетворенням коду. Вбудований налагоджувач може працювати і налагоджувачем рівня вихідного коду, і відладчиком машинного рівня. Інші вбудовані інструменти включають редактор форм для спрощення створення графічного інтерфейсу програми, дизайнер класів і дизайнер схеми бази даних, веб-

редактору. За допомогою Visual Studio ви можете створювати та інтегрувати сторонні доповнення (розширення), щоб розширити функціональність майже на кожному рівні, включаючи підтримку систем керування вихідним кодом, таких як Subversion і Visual SourceSafe, нових наборів інструментів та кодово-орієнтовані мови програмування або інструментами для інших аспектів процесу розробки ПЗ (наприклад, клієнт Team Explorer для роботи з Team Foundation Server). [21-22]

2. Python (найчастіше вживане прочитання — «Пайтон» — інтерпретація мови програмування високого рівня на основі об'єктів із сильною динамічною типізацією. Розроблено Гвідо ван Россумом у 1990 році. Високоякісні структури даних у поєднанні з динамічною семантикою та динамічним підключенням роблять його привабливим для швидкої розробки програмного забезпечення та інструментом для інтеграції існуючих компонентів. Python підтримує модулі та пакети модулів і заохочує модульність і повторне використання коду. Інтерпретатор Python і користувацькі бібліотеки доступні як у скомпільованих, так і в збережених форматах на всіх основних платформах. Мова програмування Python підтримує різноманітні шаблони програмування, включаючи тему, метод, функцію та сторінку. Із переваг Python можна визначити:

- чистий синтаксис (для виділення блоків необхідно використати відступи);
- переносність програм (притаманно інтерпретованим мовам);
- стандартний дистрибутив має багато корисних модулів (включаючи модуль для розробки графічного інтерфейсу);
- можливість використовувати Python в інтерактивному режимі (дуже корисно для випробування та вирішення простих завдань);
- просте, але водночас дуже потужне середовище розробки під назвою IDLE, написане на Python;
- зручний для вирішення математичних завдань (може працювати з комплексними числами, може працювати з цілими числами будь-якого розміру, може використовуватись як потужний калькулятор у режимі розмови);

- Open Source (можливість редагування спільно з іншими користувачами). [19-20]

3. Microsoft Excel (офіційна назва Microsoft Office Excel) — табличний процесор, програма для електронних таблиць, розроблена Microsoft для Microsoft Windows, Windows NT і Mac OS. Програма є частиною пакету Microsoft Office.

Типове використання Excel:

- оскільки електронний лист Excel є електронною таблицею, він часто використовується для створення документів без різноманітних розрахунків у звичайному форматі електронних таблиць (наприклад, розклади чи прайс-листи в магазинах). В Excel дуже просто можна створювати різні види діаграм чи графіків, які братимуть дані для побудови із осередків таблиці (графік зниження ваги тіла за вказаний період часу від початку занять спортом);
- Excel доступний для використання рядовим користувачам для елементарних розрахунків (скільки витратив за цей місяць);
- В Excel міститься велика кількість математичних і статистичних функцій, через що його можуть використовувати учні навчальних закладів для розрахунків курсових, лабораторних робіт;
- Excel дуже популярний для бухгалтерії — у більшості компаній це основний інструмент для формування звітів, розрахунків і створення діаграм. Звичайно, він має в собі відповідні функції;
- Excel навіть може працювати базою даних (краще використовувати спеціалізовані програми для створення баз даних, бо Exsel до повноцінної бази даних далеко). [31]

2.3.2. Написання коду програми

Для побудови моделі порушника використовується опитувальник, питання якого записані в файлі Excel, з указаними можливими відповідями, а також відповідними порушниками, згідно до ймовірності і потенціалу. Для виведення результатів і розрахунку ймовірності і потенціалу порушника необхідно створити окремий файл Exsel на 3 таблиці – для виводу результатів, розрахунку потенціалу і ймовірності порушника (рис. 2.1 – 2.5).

```
def workbook_creation():
    Intruder_list = ['','Спеціальні служби іноземних держав','Терористичні, екстремістські угруповання',
                     'Злочинні групи (кримінальні структури)','Конкуруючі організації',
                     'Розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів',
                     "Зовнішні суб'єкти (фізичні особи)", 'Колишні працівники', 'Клієнти',  'Директор', 'Бухгалтер',
                     'Юрист', 'IT спеціаліст', 'Прибиральник', 'Охоронник']

    Result_workbook = openpyxl.Workbook()
    Result_workbook.create_sheet('Results')
    Result_workbook.create_sheet('Prob')
    Result_workbook.create_sheet('Int')

    Int_sheet = Result_workbook['Int']
    Prob_sheet = Result_workbook['Prob']

    for i in range(1, 15):
        Int_sheet.cell(row=1, column=i).value = Intruder_list[i]
        Prob_sheet.cell(row=1, column=i).value = Intruder_list[i]
        Int_sheet.cell(row = 2, column = i).value = 0
        Prob_sheet.cell(row=2, column=i).value = 0

    Result_workbook.save('D:\\Учёба\\4_course\\Result1.xlsx')
```

Рис. 2.1. Створення файлу Excel для виведення результатів і

```
def main(name):
    workbook_creation()
    syst_class = int(input("Автоматизована система якого класу на підриємстві? Написати цифру\n"))
    if syst_class ==1:
        AC = 'AC1'
    elif syst_class ==2:
        AC = 'AC2'
    elif syst_class ==3:
        AC = 'AC3'
    else:
        print('Невірний клас, введіть цифру 1, 2 або 3')
        main()
```

Рис. 2.2. Визначення класу автоматизованої

```
Log_base = openpyxl.load_workbook('D:\\Учёба\\4_course\\Data.xlsx')
Log_list = Log_base[AC]
number_of_row = Log_list.max_row + 1

for i in range(1, number_of_row):
    print(i)
    task_name = 'A' + str(i)
    type_name = 'B' + str(i)
    intruder_type_name = 'C'+ str(i)
    prob_type_name = 'D' + str(i)

    task = str(Log_list[task_name].value)
    type = str(Log_list[type_name].value)
    intruder_type = str(Log_list[intruder_type_name].value)
    prob_type = str(Log_list[prob_type_name].value)

    task_handler(task, type, intruder_type, prob_type)
```

Рис. 2.3. Зчитування інформації з відповідної таблиці файлу-опитувальника

```
def task_handler(task, type, intruder_type, prob_type):
    ans = input(task)
    if type == 'Any':
        ans = ans
    elif ans in type:
        ans = ans
    else:
        print('Введено невірно')
        task_handler(task, type, intruder_type, prob_type)

    Result_base = openpyxl.load_workbook('D:\\Учёба\\4_course\\Result1.xlsx')
    Result_list = Result_base['Results']

    number_of_row = Result_list.max_row + 1

    cell_name = 'A' + str(number_of_row)
    Result_list[cell_name] = task

    cell_name = 'B' + str(number_of_row)
    Result_list[cell_name] = ans
    Result_base.save('D:\\Учёба\\4_course\\Result1.xlsx')
```

Рис. 2.4. Отримання відповідей, перевірка на коректність та зберігання їх в файлу

```
if prob_type == 'NONE':
    pass
else:
    prob_type = prob_type.split(',')

    Result_base = openpyxl.load_workbook('D:\\Учёба\\4_course\\Result1.xlsx')
    Prob_list = Result_base['Prob']

    for type in prob_type:
        cell_name = type + '2'
        value = int(Prob_list[cell_name].value)
        print(value, ans)
        value = str(value + int(ans))
        Prob_list[cell_name] = value
    Result_base.save('D:\\Учёба\\4_course\\Result1.xlsx')
```

Рис. 2.5. Розрахунок ймовірності порушника з подальшим збереженням в створений файл

2.4. Алгоритм програми

Рис. 2.6. Алгоритм формування таблиці, сторінок для результатів і запису розрахунк в ймовірності/потенціалу порушника

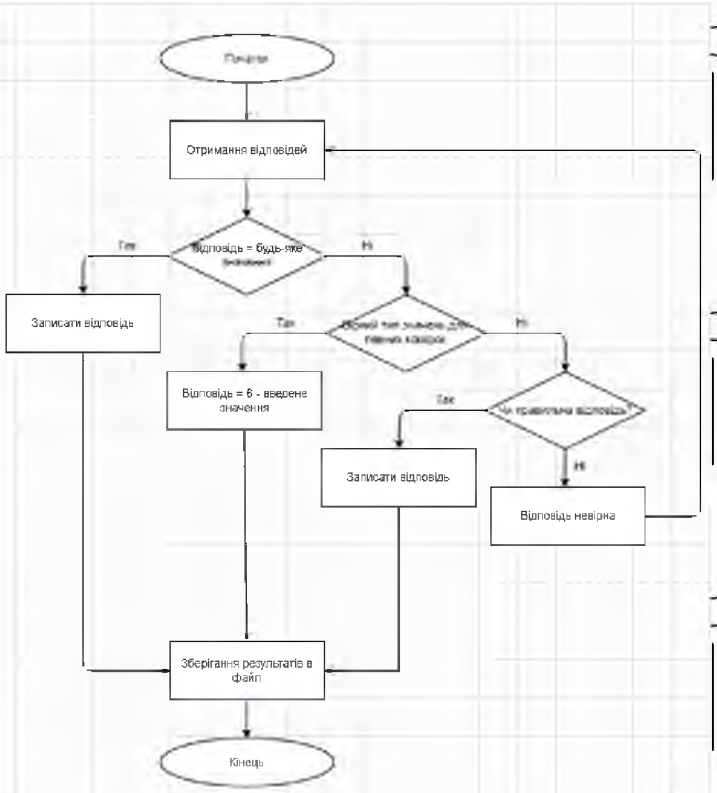


Рис. 2.7. Отримання інформації по класу АС і

звернення по певної сторінки бази даних

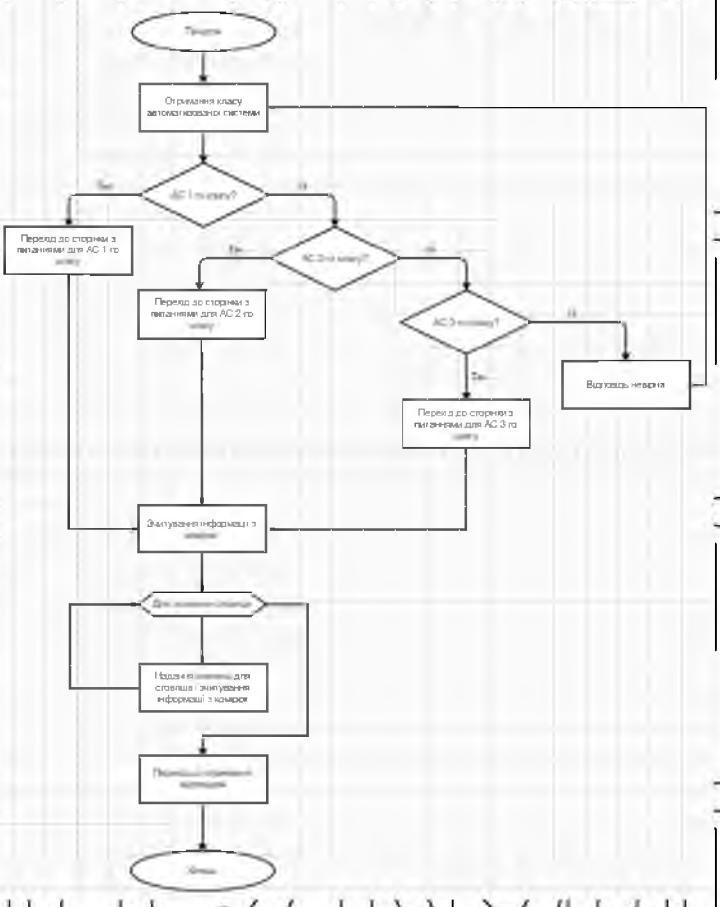


Рис. 2.8. Алгоритм отримання відповідей,

перевірка і запис до файлу

2.4. Висновки до розділу

В даному розділі було створено автоматизовано систему побудови моделі порушника.

Першим етапом було формування опитувальника, в який входили питання, які будуть задаватися особам, представляючим підприємство, і які будуть вносити інформацію по ньому. Також опитувальник має 3 додаткових пункти, які не може бачити опитуваний – ймовірні відповіді та порушники, які можуть здійснювати неправомірні дії, спрямовані на порушення інформаційної безпеки підприємства.

В розділі пояснюється, яким чином проводиться побудова автоматизованої системи, а також як опитуваний зможе ознайомитись з моделлю порушника і проаналізувати її.

РОЗДІЛ 3
ПЕРЕВІРКА РОБОТИ АВТОМАТИЗОВАНОЇ СИСТЕМИ ПОБУДОВИ МОДЕЛІ ПОРУШНИКА

3.1. Тестування автоматизованої системи

Перевірка роботи автоматизованої системи побудови моделі порушника буде проводитися в програмі Visual Studio.

Завдання експерименту – перевірка відповідності розробленої автоматизованої системи вимогам, а саме:

1. Коректна роботи форми користувача;
2. Зчитування питань з 1 файлу і запис відповідей в інший згідно до розробленого алгоритму;
3. Проведення розрахунків з введеними даними і коректний запис в файл.

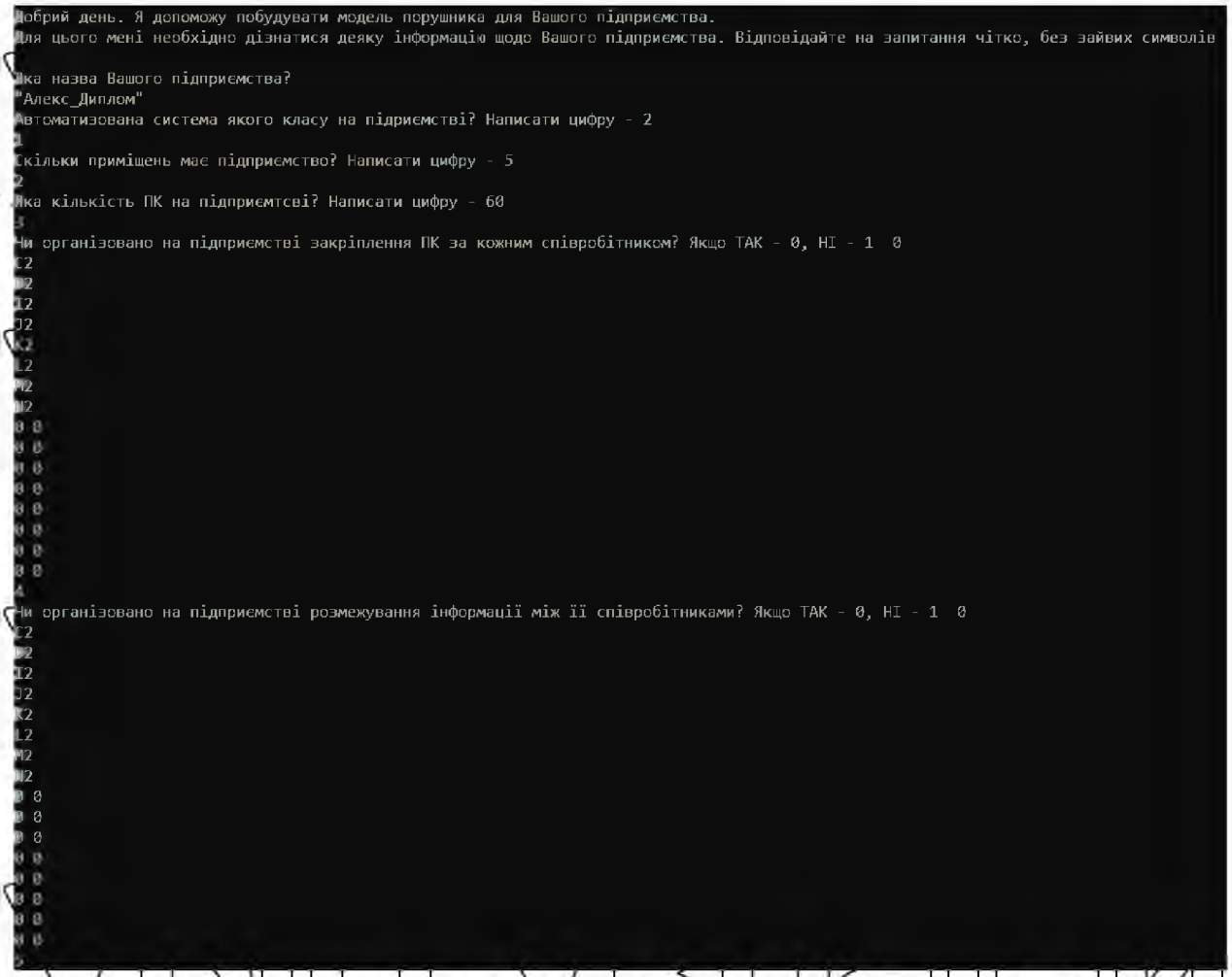


Рис. 3.1. Початок опитування

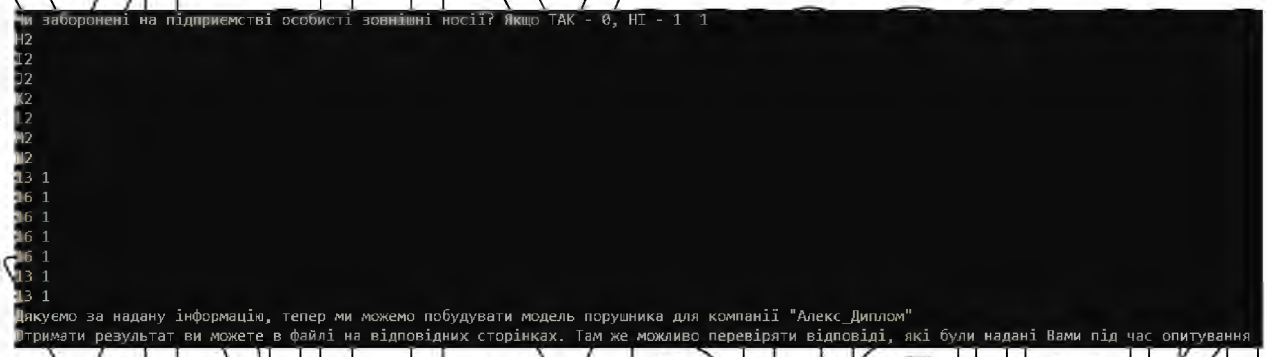


Рис. 3.2. Кінець опитування

Скільки приміщень має підприємство? Написати цифру -	5
Яка кількість ПК на підприємтсві? Написати цифру -	60
Чи організовано на підприємстві закріплення ПК за кожним співробітником? Якщо ТАК - 0, НІ - 1	0
Чи організовано на підприємстві розмежування інформації між її співробітниками? Якщо ТАК - 0, НІ - 1	0
Чи можливий доступ сторонніх до приміщень підприємства? Якщо ТАК - 1, НІ - 0	1
Необхідно вказати, яка інформація з обмеженим доступом використовується на підприємстві? Конфіденційна інформація. Якщо ТАК - 1, НІ - 0	1
Службова інформація. Якщо ТАК - 1, НІ - 0	1
Таємна інформація. Якщо ТАК - 1, НІ - 0	0
Яка секретність інформації з обмеженим доступом на підприємстві з огляду на можливі наслідки з її розповсюдженням? Без наслідків - 1, Низька - 2, Середня - 3, Висока - 4, Дуже висока - 5	3
Яка цінність інформації для функціонування підприємства? Низька - 1, Середня - 2, Висока - 3, Дуже висока - 4	2
Чи організовано на підприємстві періодична перевірка функціонування АС та її захисту? Якщо ТАК - 0, НІ - 1	0
Яка періодичність перевірок на рік? Написати цифру -	3
Чи проводиться на підприємстві навчання Політики безпеки інформації? Якщо ТАК - 0, НІ - 1	0
Чи проводиться на підприємстві перевірка знань Політики безпеки інформації? Якщо ТАК - 0, НІ - 1	0
Яка періодичність перевірок на рік? Написати цифру -	3
Чи сформовано відділ інформаційної безпеки на підприємстві? Якщо ТАК - 0, НІ - 1	0
Чи прописані процедури та заходи реагування на інциденти порушення безперервної діяльності компанії? Чи ознайомленний персонал з цією інформацією? Якщо ТАК - 0, НІ - 1	0
Які можливі втрати від ймовірного порушення безперервної діяльності компанії? Низькі - 1, Середні - 2, Високі - 3, Дуже високі - 4	3
Чи сформовано Інструкцію з організації парольного захисту? Якщо ТАК - 0, НІ - 1	0
Чи заборонені на підприємстві особисті зовнішні носії? Якщо ТАК - 0, НІ - 1	1

Рис. 3.3. Введення результатів в створений файл на сторінку результатів

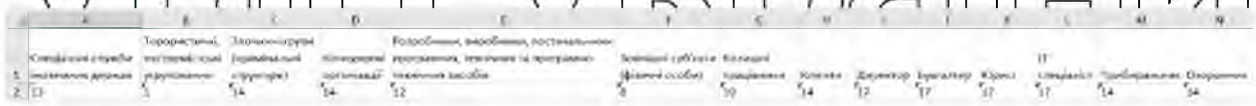


Рис. 3.4. Розрахунок ймовірності порушника

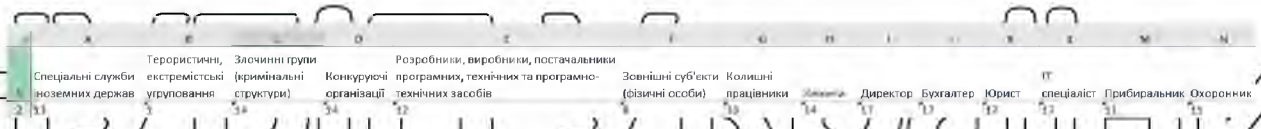


Рис. 3.5. Розрахунок потенціалу порушника

По результатам (рис. 3.3 – 3.5) ми бачимо, що підприємство має АС 2 класу та найбільший показник потенціалу і ймовірності порушника мають внутрішні

порушники, а саме директор, юрист, бухгалтер і IT спеціаліст. Найменший потенціал і ймовірність порушника у Терористичних, екстремістських угрупованнях.

Було проведено перевірку різних класів АС з різними показниками, автоматизована система побудови моделі порушника працює вірно, без помилок. Це означає, що ми можемо побудувати модель порушника для будь-якого підприємства, яка буде 1 із основних складників його інформаційної безпеки.

Порівняємо розроблену програму з автоматизованими системами з табл. 1.5.

Таблиця 3.1.

Порівняння створеної Автоматизованої системи з іншими

Критерій / Програма	Дипломна розробка	Microsoft threat modeling tool	Mozilla threat modeling tool	OWASP Threat Dragon	Threat Modeler	IriusRisk	securiCAD	SD Elements by Security Compass
Безкоштовне використання	+	+	+	+	-	-	-	-
Український інтерфейс	+	-	-	-	-	-	-	-
Зручний, сучасний дизайн	+	+	-	+	-	+	+	+
Створення моделі за допомогою анкетування	+	-	-	-	-	-	-	+
Можливість редагування	+	+	-	+	+	+	+	+
Виведення результатів в таблиці	+	-	+	-	-	-	-	-
Створення діаграм/графіків	-	+	-	+	+	+	+	+
Можливість створення моделі порушника	+	-	-	-	-	-	-	-

3.2. Висновки до розділу

В третьому розділі проводиться перевірка роботи автоматизованої системи, яка була описана в другому розділі.

Показано як відбувається опитування, де опитуваний має відповідати на питання по підприємству, яке від представляє. По цим питанням формуються ймовірності і потенціал кожного порушника – внутрішнього і зовнішнього. Проілюстровано, як вони зберігаються в файлі, який по завершенню буде передаватись відповідальній особі для створення або модернізації підприємства.

Як приклад було проведено дослідження підприємства з АС 2 класу, показано ймовірних порушників.

Порівняно розроблену автоматизовано систему з автоматизованими системами, що були надані в Розділі 1.

ВИСНОВОК

Для виконання дипломної роботи було розглянуто терміни автоматизована система, модель порушника, різновиди, можливості порушників, його ймовірні дії і принципи роботи, мету дій, також досліджено методику їх побудови. Було проаналізовано різні моделі порушника порівняно між собою по критеріям, таким як можлвість порушення ПРД, отримання статусу авторизованого користувача, використання позаштатних пристроїв, використання недостатньої якості інформаційно-уразливих режимів, функцій і послуг, що надаються АС, та можливе виведення з робочого стану тощо. Саме ці критерії і слугували основою для розробки автоматизованої системи.

Було проведено дослідження по автоматизованим системам побудови моделей, описано деякі з них та порівняно між собою. Було порівняно такі автоматизовані системи, як: Microsoft threat modeling tool, Mozilla threat modeling tool, OWASP Threat Dragon, MyAppSecurity, MyAppSecurity, securiCAD, IriusRisk, SD Elements by Security Compass – як моделі загроз.

Завдяки проаналізованим джерелам і отриманій інформації в подальшому стала можлива розробка власної автоматизованої системи побудови моделі порушника. Система базується на опитувальнику, завдяки якому можна буде отримати інформацію про підприємство, згідно до якої в результаті буде сформовано модель порушника, де вказуються ймовірні порушники з ймовірністю загроз від кожного з них.

Автоматизована система написана на мові програмування Python та з використанням таких програм як Microsoft Excel та Visual Studio 2019. Microsoft Excel використовувався як база даних, звідки брались питання і куди в подальшому записуються відповіді і проводиться автоматичний розрахунок ймовірностей порушника.

Після створення автоматизованої системи побудови моделі порушника, вона була порівняна з іншими автоматизованими системами, та стало зрозуміло, що вона

не поступається іншим, а також, так як ця система має україномовний інтерфейс, вона буде мати великий попит на українському ринку.

Відповідно до проведеного тестування автоматизованої системи можна дійти до висновку, що система працює вірно, і, завдяки цій системі, підприємства, які в подальшому будуть користуватися послугами розробки, матимуть можливість використовувати отриману модель порушника при формуванні чи модернізації своєї Системи інформаційної безпеки підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богуш В.М., Юдін О.К. Інформаційна безпека держави. –К.: «МК-Прес», 2005. - 432с., іл.
2. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. ДСТСЗІ СБ України, 2000
3. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України, 1999
4. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування Основні положення. ДСТСЗІ СБ України, 1999
5. НД ТЗІ 3.7-003 -2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. ДСТСЗІ СБ України, 2005
6. Про захист інформації в інформаційно-комунікаційних системах: Закон України № 1089-IX від 16.12.2020
7. Методика оцінки загроз для інформації автоматизованих систем / Микола Будько // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2005. – Вип. 10. – С. 35-46. – Бібліогр.: 5 назв.
8. Комаров М. Ю. Аналіз і дослідження загроз для захищеного вузла інтернет доступу / М. Ю. Комаров, С. Ф. Гончар // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Технічні науки. - 2018. - Т. 29(68), № 4(1). - С. 165-168. - Режим доступу: http://nbuv.gov.ua/UJRN/sntuts_2018_29(68)_4(1)__29.
https://er.nau.edu.ua/bitstream/NAU/50798/1/%d0%a4%d0%9a%d0%9a%d0%9f%d0%86_2020_123_%d0%a6%d0%b0%d1%80%d0%b5%d0%bd%d0%ba%d0%be%d0%92.%d0%92..pdf

9. Лопатников Л. И. Экономико-математический словарь: Словарь современной экономической науки / Л. И. Лопатников — 5-е изд., перераб. и доп. — М.: Дело, 2003. — 520 с.

10. Красов, А.В. Методика построения системы обнаружения вторжений для voip-трафика/А.В. Красов, Д.И. Кириллов //63-я научнотехническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов СПбГУТ. – СПб.: СПбГУТ, 2011, т1. – С.248-249.//Фундаментальные исследования. – 2014 – № 8(часть 6). – С. 1300-1308.

11. L.A.Gordon and M.P.Loeb, “The Economics of Information Security Investment, ”ACM Transactions on Information and System Security, vol.5, no. 4, pp.438–457, 2002.

12. М.Г. Медведєв і І.О.Пащенко, Теорія ймовірностей та математична статистика, Київ, Ліра-К, 2008

13. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Харків: Форт, 2010. 593с

14. Мокренко П.В. Елементи і пристрої фізичної та електронної охорони об’єктів. Львів, 2000.

15. Петраков А. В., Дорошенко П. С., Савлуков Н. В. Охрана и защита современного предприятия. М., 1999.

16. Електронний ресурс – Режим доступу до ресурсу: https://studfile.net/preview/16435780/ (5 травня 2022)

17. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT)

18. Електронний ресурс – Режим доступу до ресурсу: https://dmee.ru/docs/100/index-2133.html (20 квітня 2022)

19. Електронний ресурс – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Python (20 квітня 2022)

20. Guido van Rossum, Python Reference Manual, release 2.4.4, 18 October 2006.

21. Електронний ресурс – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Microsoft_Visual_Studio#Visual_Studio_2019 (13 травня 2022)
22. Visual Studio 2019 Compatibility | Microsoft Docs. 2019.
23. Електронний ресурс – Режим доступу до ресурсу: https://elearning.sumdu.edu.ua/free_content/lectured:de1c9452f2a161439391120eef364dd8ce4d8e5e/20160217112601/183252/index.html (13 травня 2022)
24. Електронний ресурс – Режим доступу до ресурсу: https://grand-sb.ru/blog/model-narushitelya-informacionnoj-bezopasnosti.html (13 травня 2022)
25. ИТ РИСКИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. // Современные наукоемкие технологии. – 2014. – №7. – С. 183–185
26. Електронний ресурс – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool (13 травня 2022)
27. Електронний ресурс – Режим доступу до ресурсу: https://owasp.org/www-project-threat-dragon/ (13 травня 2022)
28. Електронний ресурс – Режим доступу до ресурсу: https://rocketreach.co/myappsecurity-profile_b5d48bcbf42e3805 (13 травня 2022)
29. Електронний ресурс – Режим доступу до ресурсу: https://foreseeti.com/securicad-enterprise/ (13 травня 2022)
30. Електронний ресурс – Режим доступу до ресурсу: https://cybersecurity-excellence-awards.com/candidates/sd-elements/ (13 травня 2022)
31. Електронний ресурс – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Microsoft_Excel (17 травня 2022)

Додаток А

ПРОГРАМНИЙ ЛІСТИНГ

```
print("Добрий день. Я допоможу побудувати модель порушника для Вашого підприємства. \nДля цього
мені необхідно дізнатися деяку інформацію щодо Вашого підприємства. Відповідайте на запитання
чітко, без зайвих символів\n")

import openpyxl

def workbook_creation():
    Intruder_list = ['','Спеціальні служби іноземних держав','Терористичні, кстремістські
угруповання',
                     'Злочинні групи (кримінальні структури)','Конкуруючі організації',
                     'Розробники, виробники, постачальники програмних, технічних та програмно-
технічних засобів',
                     "Зовнішні суб'єкти (фізичні особи)", 'Колишні працівники', 'Котлети',
'Директор', 'Бухгалтер',
                     'Юрист', 'IT спеціаліст', 'Прибиральник', 'Охоронник']
    Result_workbook = openpyxl.Workbook()
    Result_workbook.create_sheet('Results')
    Result_workbook.create_sheet('Prob')
    Result_workbook.create_sheet('Int')

    Int_sheet = Result_workbook['Int']
    Prob_sheet = Result_workbook['Prob']

    for i in range(1, 15):
        Int_sheet.cell(row=1, column=i).value = Intruder_list[i]
        Prob_sheet.cell(row=1, column=i).value = Intruder_list[i]
        Int_sheet.cell(row = 2, column = i).value = 0
        Prob_sheet.cell(row=2, column=i).value = 0

    Result_workbook.save('D:\\Учёба\\4 course\\Result1.xlsx')

def task_handler(task, type, intruder_type, prob_type):
    ans = input(task)
    if type == 'Any':
        ans = ans
    elif 'Rev' in type:
        ans = 6 - int(ans)
    elif ans in type:
        ans = ans
    else:
        print('Введено невірно')
        task_handler(task, type, intruder_type, prob_type)

    Result_base = openpyxl.load_workbook('D:\\Учёба\\4 course\\Result1.xlsx')
    Result_list = Result_base['Results']

    number_of_row = Result_list.max_row + 1

    cell_name = 'A' + str(number_of_row)
    Result_list[cell_name] = task

    cell_name = 'B' + str(number_of_row)
```

```
        Result_list[cell_name] = ans

    Result_base.save('D:\\Учёба\\4_course\\Result1.xlsx')

    if intruder_type == 'NONE':
        pass
    else:
        intruder_type = intruder_type.split(',')

        Result_base = openpyxl.load_workbook('D:\\Учёба\\4_course\\Result1.xlsx')
        Int_list = Result_base['Int']

        for type in intruder_type:
            cell_name = type + '2'
            print(cell_name)
            value = int(Int_list[cell_name].value)
            value = str(value + int(ans))
            Int_list[cell_name] = value

        Result_base.save('D:\\Учёба\\4_course\\Result1.xlsx')

    if prob_type == 'NONE':
        pass
    else:
        prob_type = prob_type.split(',')

        Result_base = openpyxl.load_workbook('D:\\Учёба\\4_course\\Result1.xlsx')
        Prob_list = Result_base['Prob']

        for type in prob_type:
            cell_name = type + '2'
            value = int(Prob_list[cell_name].value)
            print(value, ans)
            value = str(value + int(ans))
            Prob_list[cell_name] = value
        Result_base.save('D:\\Учёба\\4_course\\Result1.xlsx')

def main(name):
    workbook_creation()
    syst_class = int(input("Автоматизована система якого класу на підприємстві? Написати цифру - "))
    if syst_class ==1:
        AC = 'AC1'
    elif syst_class ==2:
        AC = 'AC2'
    elif syst_class ==3:
        AC = 'AC3'
    else:
        print('Невірний клас, введіть цифру 1, 2 або 3')
        main()

    Log_base = openpyxl.load_workbook('D:\\Учёба\\4_course\\Data.xlsx')
    Log_list = Log_base[AC]
    number_of_row = Log_list.max_row + 1

    for i in range(1, number_of_row):
        print(i)
        task_name = 'A' + str(i)
        type_name = 'B' + str(i)
        intruder_type_name = 'C'+ str(i)
        prob_type_name = 'D' + str(i)
```

```
        task = str(Log_list[task_name].value)
        type = str(Log_list[type_name].value)
        intruder_type = str(Log_list[intruder_type_name].value)
        prob_type = str(Log_list[prob_type_name].value)

        task_handler(task, type, intruder_type, prob_type)


if __name__ == '__main__':
    name = input("Яка назва Вашого підприємства?\n")
    main(name)

print("Дякуємо за надану інформацію, тепер ми можемо побудувати модель порушника для компанії",
name + "\nОтримати результат ви можете в файлі на відповідних сторінках. Там же можливо
перевіряти відповіді, які були надані Вами під час опитування")
```

СЛАЙДИ ПРЕЗЕНТАЦІЇ

АКТУАЛЬНІСТЬ

Із преходом в інформаційну епоху найважливішим ресурсом стала інформація. Для ведення ефективної боротьби з порушниками, якы мають змогу обійти захисні засоби та для ефективного захисту інформації фахівцями було розроблено та запропоновано різні види моделей, зокрема, для початкового прогнозування ризиків і втрат пов'язаних із веденням інформаційного протиборства і модель порушника

Модель порушника представляє собою опис можливих дій порушника, який складається на підставі детального аналізу можливих загроз, способів та каналів їх реалізації, а також типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Така модель будується для розробки комплексу заходів для забезпечення безпеки алгоритму.

Продовження додатку Б

МЕТА РОБОТИ

Метою роботи є розробка власної автоматизованої системи побудови моделі порушника для підприємств

Для досягнення мети необхідно виконати такі задачі:

- Проаналізувати існуючі автоматизовані системи побудови моделей;
- Дослідити моделі порушника і способи побудови моделей;
- Розробити автоматизовану систему побудови моделі порушника
- Провести експериментальне дослідження автоматизованої системи для перевірки коректності її роботи

НОВИЗНА

Удосконалено процес побудови моделі порушника, що за рахунок автоматизації результатів анкетування підприємства, можливості вибору АС різних класів та використання україномовного інтерфейсу дозволяє спростити процес побудови КСЗІ на підприємстві.

Продовження додатку Б

ОБ'ЄКТ, ПРЕДМЕТ, ПРАКТИЧНА ЦІННІСТЬ ДОСЛІДЖЕННЯ

Об'єкт дослідження – процес побудови моделей порушника

Предмет дослідження – автоматизована система побудови моделей

Практична цінність розробки є створення автоматизованої системи, якій немає аналогів, завдяки якій спрощується процедура побудови моделі порушника

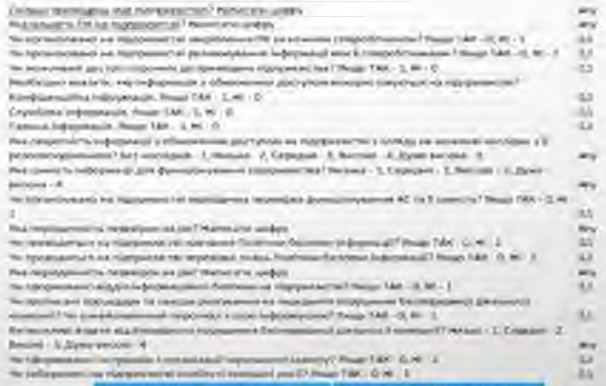
АНАЛІЗ ІСНУЮЧИХ АВТОМАТИЗОВАНИХ СИСТЕМ ПОБУДОВИ МОДЕЛЕЙ

Критерій / Програма	MicrosoR threat modeling tool	[illegible]	OWASP Threat Dragon	Threat Modeler	IriusRisk	securiCAD	SD Elements by Security Compass
Безкоштовне використання	+	+	+				
Український інтерфейс							
Зручний, сучасний дизайн	+		+		+	+	+
Створення моделі за допомогою анімування							+
Можливість редагування	+		+	+	+	+	+
Виведення результатів в таблиці		+					
Створення діаграм/графіків	+		+	+	+	+	+
Можливість створення моделі порушника							

Продовження додатку Б

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ

Для побудови моделі порушника використовується опитувальник, питання якого записані в файлі excel, з указаними можливими відповідями, а також відповідними порушниками, згідно до ймовірності і потенціалу. Для виведення результатів і розрахунку ймовірності і потенціалу порушника необхідно створити окремий файл exsel на 3 таблиці – для виводу результатів, розрахунку потенціалу і ймовірності порушника



Отриманий результат дослідження	Потенціал/ймовірність порушника
0-5	найнижчий
5-10	низький
10-20	середній
20+	високий

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ

Створення файлу Excel для виведення результатів і розрахунків

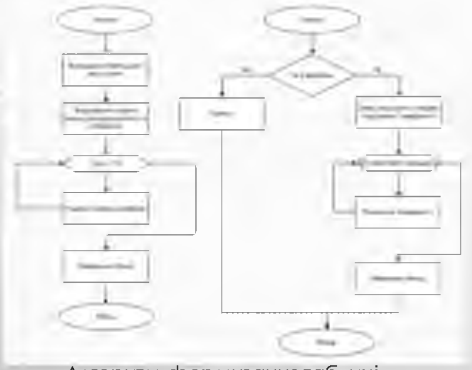
Отримання відповідей, перевірка на коректність та зберігання їх в файлу

Зчитування інформації з відповідної таблиці файлу-опитувальника

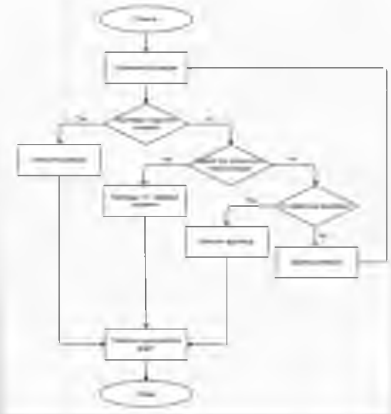
Визначення класу автоматизованої системи

Розрахунок ймовірності порушника з подальшим збереженням в створений файл

АЛГОРИТМ РОБОТИ АВТОМАТИЗОВАНОЇ СИСТЕМИ



Алгоритм формування таблиці, сторінок для результатів і запису розрахунків ймовірності/потенціалу порушника



Отримання інформації по класу АС і звернення до певної сторінки бази даних

Алгоритм отримання відповідей, перевірка і запис до файлу

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ

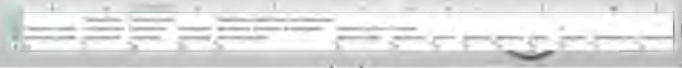
Перевірка роботи автоматизовоної системи побудови моделі порушника буде проводитися в програмі visual studio.

Завдання експерименту – перевірка відповідності розробленої автоматизованої системи вимогам, а саме:

- Коректна роботи форми користувача;
- Зчитування питань з 1 файлу і запис відповідей в інший згідно до розробленного алгоритму;
- Проведення розрахунків з введеними даними і коректний запис в файл

Початок опитування

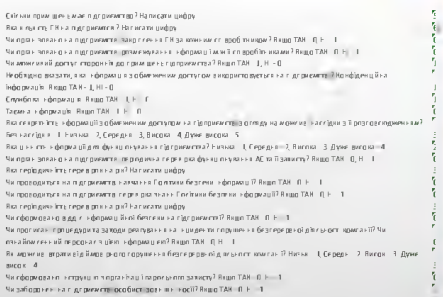
Ймовірність порушника



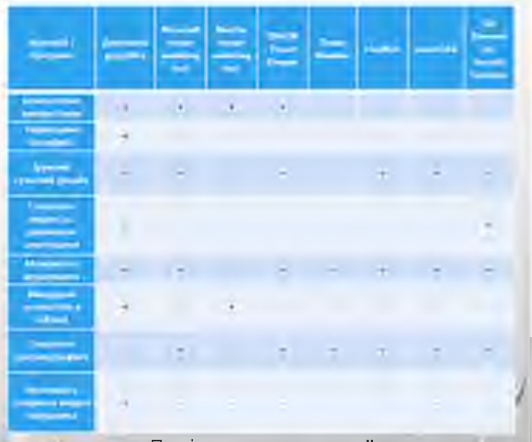
Потенціал порушника

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ

Відповідно до проведеного дослідження можна зробити висновок, що розробка працює коректно, і відповідає висунутим вимогам. Дослідження проводилось для АС 2 класу, але так саме було проведено дослідження для АС 1-го і 2-го класів. Було порівняно по критеріям з іншими автоматизованими системами, і із переваг можна побачити збір інформації шляхом анкетування, сучасний, зручний український інтерфейс, і можливість редагування



Введення результатів в створений файл на сторінку результатів



Порівняння створеної Автоматизованої системи з іншими

ВИСНОВОК

- Проведено критеріальний аналіз автоматизованих систем побудови моделей, що показало відсутність наявності автоматизованих систем побудови моделей;
- досліджено моделі порушника, методику їх побудови, що дозволило обрати концепцію побудови моделі, а саме опитувальник;
- розроблено власну автоматизовану систему побудови моделі порушника, що дало можливість автоматизувати процес. Автоматизована система, відповідно до результатів опитувальника, формує модель порушника, де вказуються ймовірні порушники і їх потенціал
- проведено експериментальне дослідження автоматизованої системи, що показало адекватність роботи автоматизованої системи.

ДЯКУЮ ЗА УВАГУ!

НУБіП України

НУБіП України

НУБіП України

НУБіП України